

UNIVERSITY OF CALIFORNIA

QUARTERLY SECURITY BULLETIN

WELCOME



This is our first quarterly security newsletter. We hope this newsletter will accomplish two important things: enhancing your security consciousness and making you aware of security clearance policy developments.

Most University clearance holders are not custodians of classified documents, and unlike custodians are not...

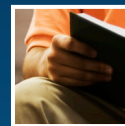
Continued on page 8

ISSUE HIGHLIGHTS



Welcome Message

1



WikiLeaks

1



Updates

2



Reporting Requirements

3



Visa Phishing Scam

4



Convicted Nuclear Spy Back in Jail

6

“Let there be light”

WIKILEAKS

As a University of California-sponsored personal security clearance holder, we want to remind you of your obligations with respect to access to and control of classified information. The reported WikiLeaks publication of thousands of State

Department documents, some labeled as “Secret”, means that certain classified documents are now accessible by individuals, world-wide. But this is not the same thing as declassification of those documents. Executive Order 13526,

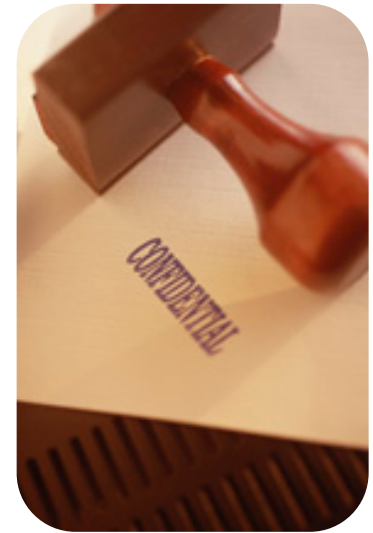
Section 1.1(4)(c) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."

As a personal security clearance holder you are knowledgeable about the access and control requirements for such documents. You cannot knowingly access classified documents for which you have no "need to know", you cannot download and possess classified documents on any computing system that does not meet federal requirements for storage of classified data, and you cannot print out classified information on paper media and store it outside of a facility meeting requirements for classified document storage.

The WikiLeaks publication of

classified State Department and, before that, DOD documents represents such an extraordinary security failure that it is clear that typical methods of document recovery and computer data sanitization will be ineffective and impractical. That leaves declassification as probably the only practical outcome. However, history has shown that any orderly review of large document holdings takes a long time.

Until we have information on what actions the Government is taking with respect to the classified status of these documents, personal security clearance holders are cautioned to avoid directly accessing or possessing the WikiLeaks documents.



"Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."

UPDATES REGARDING YOUR SECURITY CLEARANCE

A new version of the SF-86, Questionnaire for National Security Positions, has been scheduled for release in January 2011. The Office of Personnel Management (OPM) will continue to allow use of the 2008 version until October 2011. At that time, any individual completing the SF-86 will be transferred over to the new version automatically. OPM has informed us that no information previously entered into the system will be lost. However, there will be additional questions to answer. Some of the changes include detailed branch questions for questions answered "yes." This may increase the size of the SF-86; however, it should reduce the comments section. OPM

has also developed a Fair Credit Release form, which will accompany the other e-QIP signature pages. This will replace the DOE Fair Credit form you have signed in the past. Our office will keep you updated on these changes as they occur.

REPORTING REQUIREMENTS: WHAT YOU NEED TO KNOW



When you hold a security clearance, you are expected to comply with the high standards of conduct normally required of persons holding positions of trust.

Standards of conduct are set by Executive Order 12968 on Access to Classified Information. That presidential order directs that access to classified information is granted only to individuals “whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for

coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information.”

Failure to comply with the standard may cause your eligibility for security clearance or occupancy of a sensitive position to be reviewed and possibly revoked.

The concept of continuing evaluation is an important part of the personnel security process. It means you are subject to periodic reinvestigation and to a reasonable degree of monitoring by supervisors, co-workers, and security professionals between investigations. These safeguards are necessary because situations and behaviors change over time. Experience shows that individuals approved for a security clearance or position of trust sometimes fall into a pattern of unreliable or untrustworthy behavior after being granted an initial clearance.

You are expected to keep your security office informed of certain changes in your personal life or activities. For further information regarding reporting requirements, such as a complete list of those requirements, please visit the Research Security Offices website.

VISA PHISHING SCAM

Did you receive an email that looked this? If so, please be aware.

Dear Visa Card user,

In addition to our other ways of preventing, detecting, and resolving fraud, we offer Verified by Visa, a free, simple-to-use and free service that confirms your identity with an extra password when you make an online transaction.

Since January 20, 2011 we require all our customers to enroll their visa cards in the Verified by Visa program. If you do not do so you will not be able to shop online with your visa card. This is a reminder to activate the Verified by Visa feature for your card as soon as possible. Click here to activate your account. We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you. We apologize for any inconvenience.

Sincerely,

Visa Inc.

The Office of Charge Card Management contacted Visa and received the following information with regard to informing its cardholders of this scam.

This email claims to be from credit card provider, Visa and instructs recipients to follow a link to activate "Verified by Visa" security protection on their card. However, in spite of the seemingly genuine logos and

Definition:

Security Clearance

A determination by an official with specified authority that an individual is trustworthy to have access to classified information or material

Definition:

Security Incident

Any incident involving classified information in which there is a deviation from the requirements of governing security regulations. Examples are compromise, inadvertent disclosure, and need-to-know violation.

Definition:

Suitability

A person's fitness based on character and reputation, for employment by the Federal Government.

formatting in the message, it does not originate from Visa. Instead it is a phishing scam intended to steal financial information. Those who do click on the link in the message will be directed to a fake website designed to closely resemble a genuine Visa web page. The fake site will request details about the cardholder's account, which can then be harvested by the scammers running the phishing operation. In this way the scammers can gain all the data they require to use the compromised card for fraudulent transactions.

Phishing scam attacks that use very similar tactics have been launched a number of times over the last few years.

Ironically, "Verified by Visa" is a genuine security program designed to protect consumers from credit card fraud. Cardholders are able to activate the security program by providing a credit card number on a secure Visa web page. The scammers have capitalized on this genuine program by diverting victims to a totally bogus activation process.

If you receive an email that appears to be from your card issuer requesting financial information or any other personal data:

- * Treat the email with suspicion.
- * Do not reply to the email or respond by clicking on a link within the email message.
- * Contact your card issuer as soon as possible to report the suspicious email. Use the number or Web site address on the back of your card or on your monthly statement.

In fact, you should be suspicious of any unsolicited email that asks you to click a link and provide personal or financial information. Phishing scammers continually target many financial institutions such as banks and credit card providers.

Visa has published information on its website regarding phishing and other scams such as this.



“Phishing: If you suspect deceit, hit delete!”

CONVICTED NUCLEAR SPY VANUNU BACK IN JAIL

The Yeshiva World, 23 May 2010: Convicted nuclear spy Mordechai Vanunu has been found guilty of contacting foreign agents, a violation of his parole, and has been sentenced to three months imprisonment. Vanunu already served 18 years in an Israeli prison after he divulged classified information regarding Israel's nuclear program to British journalists. In his latest case, he told the court that the country has not succeeded in changing his views that imprisoned him for 18 years, so there is no chance of teaching him a lesson by putting him behind bars for an additional three months. The former nuclear technician passed information to the British press in 1986, and after luring him to Italy, Mossad agents took him into custody, where he stood trial behind closed doors, sentenced to 18 years, 11 of which were served in solitary confinement. His release was accompanied by many travel and other restrictions, including media interviews and contacting foreigners, however, the defiant Vanunu continues to spurn the Israeli judicial system. He worked at the Negev nuclear research and weapons center for nine years as a manager and then moved to the Dimona nuclear facility. In the late 1980s he announced his conversion to Christianity, and eventually became infamous in Israel with his disclosure of classified material surrounding Israel's nuclear program.



Source: <http://www.theyeshivaworld.com/news/General+News/58897/Convicted-Nuclear-Spy-Vanunu-Back-in-Jail.htm>

DID YOU KNOW?



We are on the web! You can find information regarding your security clearance such as reporting requirements, foreign travel information, view our briefings and so much more at the click of a button.

Visit us at: <http://labs.ucop.edu/security/index.html>

SECURITY CHALLENGE POP QUIZ!

Test your knowledge on personnel security and information security issues.

1. The Personnel Security program has _____ adjudicative guidelines for determining eligibility for access to classified information.
2. What is the minimum, initial investigation type required for an employee requiring access to Top Secret or "Q" level information?
3. How many classification categories are there for National Security information?
4. This Executive Order sets the U.S. government policy for classifying national security information that must be protected from unauthorized disclosure.
5. The standards set by this Executive Order directs that access shall be granted only to individuals "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."
6. Employees holding a Top Secret or "Q" clearance must be reinvestigated every ___ years.
7. Access to National Security information is not granted until the information security indoctrination briefing is successfully concluded and the subject completes the required _____ nondisclosure form.



Answers can be found on the following page

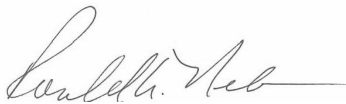
Welcome message continued from page 1...

constantly reminded of their security obligations. Nevertheless as a clearance holder you need to keep security clearly in mind. This newsletter contains stories and articles we hope will help you make security a priority in your life.

As you are aware, obtaining and maintaining a security clearance is an intrusive and complex process. We want to keep you informed of policy developments as we learn of them. This may not make compliance with new requirements pleasant or easier, but avoiding a surprise may make compliance less stressful for you.

In closing, we hope you enjoy our newsletter. Also, we want to hear from you about what is useful and what is not. So please let us know what you think about this and future newsletters so that we can make this an effective tool.

Sincerely,



Ronald Nelson
Research Facility
Security Officer



Brandi Marotta
Assistant Research Facility
Security Officer

FINAL THOUGHT...

If you would like to see us address a particular topic, process, or guideline in a future newsletter, please submit your request to the Research Security office at Brandi.Marotta@ucop.edu



Pop Quiz Answers!

1. 13
2. SBI
3. 3
4. E.O. 13526
5. E.O. 12968
6. 5
7. SF-312